

1 a number of security protocols, including spam filters, firewalls, and email gateways. I have
2 performed infrastructure security risk assessments in ten countries.

3 4. I have served as an expert consultant or expert witness for the U.S. Government in
4 approximately ten cases, and I have served as an expert consultant or expert witness for the
5 defendant in several criminal cases and half-a-dozen civil cases.

6 5. A unique Internet Protocol (“IP”) address is assigned by an Internet Service Provider
7 (“ISP”) to each network connection directly using the ISP’s services.

8 6. I have been engaged to assist Henry and Carole Klyce in identifying the cause and
9 source of takeovers of each of their email accounts.

10 7. Carole has an email account at Yahoo! She lives in Piedmont, California, and the IP
11 address of the computer she typically uses can be associated with that location. On inspection of
12 her account’s security information, we observed that at some point in time, a 917 area code
13 telephone number was associated with this account by someone, but 917 is not a California area
14 code; it is an area code in New York. There were also account recovery questions and answers
15 supplied for the account which Carole told me she did not recognize. Henry Klyce has an email
16 account at AOL. On inspection of his account’s security information, we observed an account
17 security question the answer to which Henry did not know, and we were unable to reset this
18 question using the “forgot security question” flows. We believe that the unauthorized values for
19 the questions and answers on both accounts are the result of unauthorized modifications to the
20 account details by unknown intruder(s).

21 8. Whenever a person uses or attempts to use an Internet service, their IP address is used
22 to communicate with the provider of that service. Accordingly, Yahoo! has business records
23 reflecting the IP address of whomever had logged onto Carole Klyce’s email account, including
24 the IP address of unauthorized intrusions and unsuccessful intrusion attempts.

25 9. Because I am employed by Yahoo! I am familiar with its privacy policies. I am aware
26 that Yahoo! will not voluntarily disclose – even to the account holder – the IP address of any
27 person or entity who logged on (or attempted to log on) to a particular account. Nor will it
28

1 voluntarily disclose other data pertinent to that account, such as account recovery information
2 (e.g. password questions and answers) known to it, or alternative communication channel data
3 (such as other email addresses or telephone numbers). The only way to obtain any of the
4 information covering this period from Yahoo! regarding a particular customer account is to
5 subpoena it pursuant to a court order. My understanding is that AOL has the same requirement.

6 10. Once the IP address of an unauthorized intruder has been disclosed by Yahoo!
7 pursuant to court order, the intruder's ISP can be identified from that IP address. One can then
8 ascertain the actual identity of the intruder by serving a court-ordered subpoena on the intruder's
9 ISP for information and documents identifying their customer then assigned that particular IP
10 address. By the same token, if a telephone number is associated with an account takeover, the
11 identity of the intruder can be determined from a telephone carrier through a court-ordered
12 subpoena seeking the identification and detailed billing records of the customer who has been
13 assigned that particular phone number. Detailed billing records or geolocation records of the
14 telephone handset may be needed to determine the identity of the customer based on the usage of
15 the phone when there is no accountholder information (for example, for a prepaid cell phone or
16 other pay-as-you-go service).

17 11. I am familiar with the security practices of other ISPs and telecommunications
18 companies. In the course of my work, I have spoken with security personnel at innumerable
19 companies over the years regarding their procedures for responding to legal process, including
20 subpoenas, seeking private customer information. Based on that experience, I can say with
21 substantial certainty that neither an ISP nor a telephone carrier would disclose the physical
22 identity and address of a customer assigned a given IP address or assigned a given telephone
23 number without service of a court-ordered subpoena, and in many cases, generally, and in this
24 case in particular this is the only way of determining the identity or location of the computer
25 abuser(s) involved.

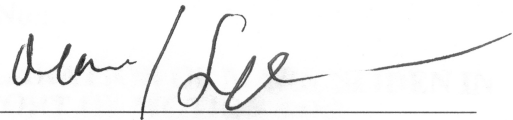
26 12. Time is of the essence in requesting information from providers of Internet services
27 because the retention period varies among providers and for different kinds and levels of detail in
28

1 data. This inconsistency is due to the high volumes of data collected, the absence of standard
2 requirements for retention, and provider concerns about subscriber privacy.

3 13. Email sent using an account on AOL or on Yahoo is typically saved automatically in
4 a "Sent Mail" folder, where it can be subsequently reviewed unless deleted. Deleted mails are
5 moved to a Trash bin folder where they may be reviewed until the provider automatically deletes
6 them permanently or the user requests immediate permanent deletion.

7 I declare under penalty of perjury under the laws of the State of California that the
8 foregoing is true and correct.

9 Executed this 5 day of May, 2011.

10
11
12 

13 Mark Seiden
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28